Listing of Claims

1. (Currently Amended)   A system for <u>positively</u> identifying an individual over a communication network; comprising:

a User that needs to be identified in e-commerce;

a Central-Entity that provides digital identity, <u>including a dynamic, non-predictable and time dependent SecureCode,</u> to the Users to positively identify themselves in e-commerce;

an External-Entity offering goods or services and needs to authenticate the Users in e-commerce based on User's digital identity;

a communication network for the User, the Central-Entity and the External-Entity to send and receive information between each other;

whereby the External-Entity forwards digital identity received from [[a]] <u>the</u> User to the Central-Entity for ~~authentication~~ <u>authenticating the User's identity</u>; and

wherein the User does not require use of software received from the Central-Entity, or a personal identity card to employ digital identity.

2. (Currently Amended) The system according to claim 1, wherein said digital identity includes <u>a combination of the</u> SecureCode and ~~other~~ <u>user-specific</u> information ~~such as UserName~~.

3. (Canceled) The system according to claim 2, wherein said SecureCode is a dynamic, non-predictable and time dependent alphanumeric code, secret code, PIN or other code.

4. (Original)   The system according to claim 1, wherein said communication network includes Internet, wireless and private networks.

5. (Currently Amended)   A method for <u>positively</u> identifying ~~an individual~~ <u>and authenticating a user</u>; comprising the steps:

The user registers at ~~the~~ <u>a</u> Central-Entity;

The user provides his personal and/or financial information to the Central-Entity;

The user receives his unique UserName and Password from the Central-Entity;

2

The user attempts to get access to a restricted web site or to buy goods and/or services from an External-Entity;

The External-Entity requests the user to authenticate himself using his digital identity;

The user requests SecureCode from the Central-Entity;

The Central-Entity generates dynamic, non-predictable and time dependable SecureCode for the user;

The Central-Entity stores a copy of the SecureCode and sends out the SecureCode to the user over a communication network;

The user receives the SecureCode over a communication network;

The user submits his a combination of his UserName and SecureCode as part of the digital identity in response to External-Entity's request;

The External-Entity forwards the user's digital identity along with the identification and authentication request to the Central-Entity over a communication network;

The Central-Entity retrieves the user's digital identity including the SecureCode from the System;

The Central-Entity compares the retrieved user's digital identity with the digital identity received from the External-Entity;

The Central-Entity sends approval identification and authorization message to the External-Entity when the digital identity forwarded to the Central-Entity, matches the user's digital identity retrieved from the system;

The Central-Entity sends a denial identification and authorization message to the External-Entity when the digital identity forwarded to the Central-Entity does not match the user's digital identity retrieved from the system; and

wherein the user is not required to use software received from the Central-Entity to employ the digital identity.

6. (Amended) The system according to claim 1, wherein the Central Entity corresponds to a Bank or other financial institution, and the User receives the digital identity from the Bank or other financial institution.

7. (Amended) The method of claim 5, wherein the Central Entity corresponds to a Bank or other financial institution, and the User receives the digital identity from the Bank or other financial institution.

8. (New)   A method for positively identifying a user based on digital identity, comprising:

A user creating an account with a trusted Central-Entity, the Central-Entity providing the user with a unique Username and Password;

The user contacting an External-Entity to conduct a transaction with the External-Entity;

The External-Entity requesting a digital identity from the user;

The user submitting their unique UserName and password to the Central-Entity for verification along with a request for digital identity;

Upon receipt of a valid UserName and password, the Central-Entity calculating a digital identity that includes a dynamic, non-predictable and time dependent SecureCode, and providing the digital identity to the user;

The user submitting their digital identity to the External-Entity for authentication; and

The External-Entity positively ~~identifying~~ authenticating the ~~user~~ user's identity based on the digital identity.

9. (New)   The method according to claim 8, wherein the digital identity includes a combination of the SecureCode and UserName.

10. (New)   The method according to claim 8, further including the user submitting their digital identity to the External-Entity for positive identification and access to a restricted web site.

11. (New)   The method according to claim 8, further including the user submitting their digital identity to the External-Entity for positive identification and payment.

12. (New)   The method according to claim 8, further including the External-Entity positively identifying the user by submitting the digital identity to the Central-Entity for approval.

4

13. (New)   The method according to claim 8, wherein the Central Entity corresponds to a financial institution, and the User receives the digital identity from the financial institution.

14. (New)   The method according to claim 13, further including the External-Entity positively identifying the user by submitting the digital identity to the financial institution for approval.

15. (New)   The system according to claim 6, wherein the financial institution is a bank.

16. (New)   The method according to claim 7, wherein the financial institution is a bank.

17. (New)   The method according to claim 13, wherein the financial institution is a bank.

18. (New)   The system of claim 2, where the user-specific information includes an identification phrase.

19. (New)   The method of claim 5, where the unique UserName includes an identification phrase.

20. (New)   The method of claim 9, where the unique UserName includes an identification phrase.